Appl. No.: Chee-Seng Chow, et al.
Amdt. dated 05/10/2005
Reply to Office action of 02/28/2005

Amendments to the Drawings:

Applicants have submitted new drawings in light of the objection to the drawings set forth in the Official Action. Formal drawings are submitted to replace the hand-written drawings originally filed with the application. Replacement sheets are attached to this response.

Appl. No.: Chee-Seng Chow, et al.
Amdt. dated 05/10/2005
Reply to Office action of 02/28/2005

REMARKS/ARGUMENTS

Applicants appreciate the thorough review of the present application as evidenced by the Official Action. The Office Action rejects Claims 1-4, 7-14, and 17-22 under 35 USC § 102(e) as being anticipated by U.S. Patent No. 6,453,353 to Win et al. The Official Action also rejects Claims 5, 6, 15, and 16 under 35 USC § 103(a) as being unpatentable over Win in view of U.S. Patent No. 6,144,959 to Anderson et al. In light of the following remarks, Applicants respectfully submit that the claims of the present application are patentably distinguishable over the newly cited references. Replacement sheets have also been attached in light of the objection to the drawings raised in the Official Action.

Win discloses that a single sign-on may be utilized to give a user access to authorized web resources, where access to web resources is based on the user's role in the organization. Thus, users are not required to log in individually to each web resource. More specifically, the user accesses an Access Server that stores a log-in page, Authentication Client Module, and Access Menu Module. The Authentication Client Module verifies a user's name and password with a Registry Server, where the Registry Server stores information about users (*e.g.*, name, password, and locale information), resources, and roles (*e.g.*, employee, customer, distributor, *etc.*) of the users. If the name and password are correct, the Authentication Client Module reads the user's roles from the Registry Server, and then encrypts and sends this information in a cookie to the user's browser. When the user selects a resource, the browser sends an open URL request and cookie(s) to a Protected Web Server, which is protected by a Runtime Module. The Runtime Module decrypts information contained in the cookie and uses the information to verify that the user is authorized to access the resource. In addition, the resource uses the cookie to return information that is customized based on the user's name and roles.

Anderson discloses a system and method for managing user accounts in a communication network. The system is capable of using a single set of credentials to access servers that are centrally located and managed such that an administrator does not have to maintain separate accounts on a shared workstation for all users. A user logging in at a client workstation provides credentials through a log-in interface. An authentication process is employed to authenticate the user to the local client, as well as to one or more servers. The authentication process compares

Appl. No.: Chee-Seng Chow, et al.
Amdt. dated 05/10/2005
Reply to Office action of 02/28/2005

credentials contained in a request for access generated by the client to entries within a domain database. If the credentials match, the domain authentication process allows access to the server process and resources. Moreover, Anderson discloses that there may be a client that provides an administrator access to a directory services database contained within a server. For example, the directory services database may support a client workstation object, where the client workstation object may include log-in information. The log-in information could include a dynamic log-in flag that is used to indicate whether user information should be retrieved from the client workstation object to create a user account on a client. Thus, when the log-in process is initiated at the client and inspects the workstation object, the log-in process may need to identify if a user account should be created in the local access database of the client.

In contrast to the disclosures described above, independent Claims 1, 11, 21 and 22 recite a method, systems, and a machine-readable medium for performing multiple user authentications with a single sign-on by performing a first user authentication, selecting a remote server, and sending a token to the remote server that contains authentication information responsive to the first authentication and information regarding an account for the user including at least one of a new account for the user and an update to an existing account for the user. The authentication information is then decoded to induce a second user authentication.

The information regarding a new or updated account that is included in the token of the claimed invention may come in various forms. With respect to the embodiment of Figure 8 of the present application, the token may include fields, including a field for a new user flag that is set when the Intranet server detects a new user. (Page 16, lines 12-15). The embodiment depicted by Figure 9 of the present application adds the capability to transmit new or updated user profile information to the remote server. The remote server may store user profile information that may help the remote server, such as a travel reservation and book service, provide efficient service to the user (e.g., dietary choices, seating preferences, travel spending limits, etc.). Once the token is determined to be valid, the token is examined for user profile information, and the remote server may create an account for a new user or update an account for an existing user depending upon the user profile information. Thus, the multiple user

Appl. No.: Chee-Seng Chow, et al.
Amdt. dated 05/10/2005
Reply to Office action of 02/28/2005

authentication of the claimed invention not only provides a single sign-on procedure, but also provides a capacity for efficiently creating or updating user accounts at the remote server.

While Win discloses a single sign-on through an Access Server to access protected web resources, Win does not disclose sending a token to a remote server that contains authentication information responsive to a first authentication and information regarding an account for the user including at least one of a new account for the user and an update to an existing account for the user, as recited by independent Claims 1, 11, 21 and 22. Win arguably discloses that the URL request and associated cookies contain authentication information, as the cookies contain profile information and a list of the user's roles. The profile information, such as username and password, allows the user to log in to the system and is used to verify that the user is authorized to access a resource, while the roles, such as employee or supplier, define the resources that are available to the user.

However, updating the profile information of Win is only achieved when the user updates profile or locale information within the Profile Management Service of Authentication Client module, which is associated with the Access Server, not the remote resources. Therefore, updated information is not included with the cookies since updating occurs at the Access Server, as shown in Figure 4 of Win. Similarly, Win does not disclose that the cookies contain information regarding a new account for the user. Simply providing the capability of updating or adding a new account is significantly different than providing information regarding a new account or an update to an existing account with a token to a remote server, as recited by the claimed invention.

Moreover, Anderson does not cure the infirmities of Win in that Anderson also does not teach or suggest sending a token to a remote server that contains authentication information responsive to a first authentication and information regarding an account for the user including at least one of a new account for the user and an update to an existing account for the user. Although Anderson arguably discloses sending authentication information in the form of credential information, the credential information does not include information regarding a new account and/or an update to an existing account. Anderson discloses that credential information

Appl. No.: Chee-Seng Chow, et al.
Amdt. dated 05/10/2005
Reply to Office action of 02/28/2005

corresponds to username, password, log-in information for a database, a log-in script, retinal scan, or fingerprint information. Thus, the credential information is only used for authentication.

Furthermore, although Anderson discloses that a dynamic log-in flag 317 may be utilized, the flag is maintained in a directory services database 223 that is associated with a server 103A (See Figure 2A of Anderson). The log-in process 207 is initiated at a client 102A that inspects the directory services database 223 to determine whether a new user account should be created in the local access database 203 maintained in the client. In this regard, the dynamic log-in flag is not contained within a token that is sent from the client to the server, as the flag is pre-stored at the server. Therefore, the dynamic user flag is not contained within a token that is sent to the server due to the fact that the flag is already located at the server before the log-in process begins.

Thus, neither Win nor Anderson, taken individually or in combination teach or suggest including information regarding an account for the user including at least one of a new account for the user and an update to an existing account for the user in a token that is sent to a remote server, as recited by amended independent Claims 1, 11, 21 and 22. Since the independent claims are patentably distinct from the cited references, the claims that depend therefrom are also patentably distinct from the cited references for at least the same reasons since the dependent claims include each of the elements of a respective independent claim. Consequently, Applicants submit that, for at least those reasons set forth above, the rejections of the claims under 35 U.S.C. § 102(e) and 35 U.S.C. § 103(a) are overcome.

Appl. No.: Chee-Seng Chow, et al.
Amdt. dated 05/10/2005
Reply to Office action of 02/28/2005

CONCLUSION

In view of the remarks presented above, it is respectfully submitted that all of the present claims of the present application are in condition for immediate allowance. It is therefore respectfully requested that a Notice of Allowance be issued. The Examiner is encouraged to contact Applicants' undersigned attorney to resolve any remaining issues in order to expedite examination of the present application.

It is not believed that extensions of time or fees for net addition of claims are required, beyond those that may otherwise be provided for in documents accompanying this paper. However, in the event that additional extensions of time are necessary to allow consideration of this paper, such extensions are hereby petitioned under 37 CFR § 1.136(a), and any fee required therefore (including fees for net addition of claims) is hereby authorized to be charged to Deposit Account No. 16-0605.
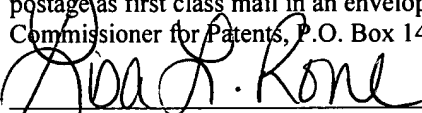
Respectfully submitted,

Trent A. Kirk
Registration No. 54,223

Customer No. 00826
ALSTON & BIRD LLP
Bank of America Plaza
101 South Tryon Street, Suite 4000
Charlotte, NC 28280-4000
Tel Charlotte Office (704) 444-1000
Fax Charlotte Office (704) 444-1111

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Mail Stop Amendment, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on May 11, 2005

Lisa Rone